INF3510 Information Security
University of Oslo
Spring 2016

Review

Audun Jøsang

General Security Concepts

- Understand information security properties/services
  - Definition of information security (ISO27001)
  - CIA (Confidentiality, Integrity and Availability) definitions
- Meaning of, and difference between other security services
  - authentication,
  - non-repudiation,
  - access control
  - auhorization
- Perspectives on security controls:
  - 3 categories of security controls: Physical, Technical, Administr.
  - Preventive, detective, corrective security controls.
  - Security controls during storage, transmission, processing.

Security Management

- Know what ISO27K series is about
- ISO27001& ISO27002
  - Title and purpose of each standard
- 20 Critical Security Controls:
  - Elements of 20 CSC,
  - Advantage over ISO27002
- Security governance and PCL (Process Capability Levels)
  - Incremental requirements for each level
  - Risk assessment as the basis for managing security
  - Metrics as basis for knowing effectiveness of controls

Risk Management

- Understand the factors that contribute to risk
  - Attacker/threat agent, vulnerability, impact
  - And how they are related: Understand diagram
- Threat scenario modelling:
  - Attacker centric, architecture centric, and asset centric
- Models for risk level estimation:
  - Qualitative
  - Quantitative
- Risk treatment strategies
  - Reduce, share, retain, avoid

Cryptography

- Symmetric ciphers
  - Parameters (block and key size) of AES
- Factors affecting the strength of ciphers and modes
  - Key length, substitution-permutation to erase statistical patterns, security by obscurity,
- MAC (Message Authentication Code)
  - Basic principle: keyed hash function
- Asymmetric ciphers
  - Understand usage of keys in encryption and digital signature
  - Digital signature, understand practical usage combined with hash
- Hybrid Crypto systems

Key Management

- Cryptoperiod = (protection period + processing period)
  - Factors affecting cryptoperiods,
  - Recommended time limit for usage of AES, RSA and ECC keys
- Key distribution problem. Understand requirements for
  - Number of keys i.c.o. symmetric and asymmetric keys.
  - Number of key distributions with and without PKI
  - Type of protection needed /confidentiality or integrity)

Computer Security

- Protection rings in microprocessor architecture
- Virtual machines
  - Understand hypervisor, VM/Guest OS, Host OS
  - Type 1 and Type 2 virtualisation architecture
  - Protection ring assignment to hypervisor, Host, VM, Apps etc.
- Security advantages of running VMs
- Security functions supported by TPM

User Authentication

- Types of authentication tokens
  - Clock-based, counter-based, challenge-response
- Password security, hashing, salting
- Biometrics systems
  - Criteria for biometric characteristics
- E-Government user authentication frameworks
  - Assurance levels
  - Assurance requirement classes
    - Authentication Method strength
    - Credential Management Assurance
    - Registration Assurance

Identity and Access Management

- Meaning of entity/identity/identifier/digital identity
- IAM phases and steps: diagram.
- Identity management models
  - Silo model / Federated model
  - Advantages and disadvantages of silo and federated models
- Facebook Connect federation scenario
- Meaning and principle of MAC, DAC, RBAC and ABAC

Communication Security

- TLS/SSL
  - Protocols
  - Key establishment
  - TLS/SSL stripping attack
- HSTS: Http Strict Transport Security
  - How it works
  - Policy enforcement
- IPSec
  - Options

Perimeter Security

- Firewall types
  - Principles of different firewalls
  - Strengths and weaknesses
  - Deep packet inspection in Next Generation Firewalls
- TLS/SSL inspection in firewalls
  - How it works
  - How to know when TSL/SSL inspection is used
- WIFI security architecture

Application Security

- What is OWASP and the top 10 vulnerabilities list
  - No need to know all 10
- Main vulnerabilities
  - SQL Injection
  - XSS - Cross-Site Scripting
  - CSRF – Cross-Site Request Forgery
  - Broken authentication and session management
- Secure Software development
  - Open SAMM Software Assurance Maturity
  - Model structure

Forensics and BCP

- The written exam has limited focus on:
  - Forensics
  - BCP (Business Continuity Planning)
- Some elements of the above topics might be superficially relevant for questions on the written exam, but the topics need not be studied in detail for the exam.

Marking Scheme

- Approximate weighing:
  - Home exam: approximately 0.4 relative weight
  - Written exam: approximately 0.6 relative weight
- You must pass both exams to pass the course!
  - E.g. score 100% on home-ex. and score 50% on written-ex. → total score 70% which normally gives mark C.
  - Score100% on home exam, and score 30% on written exam normally gives mark F.
  - Written exam indicates what you have learnt from the course
- It’s important that you don’t fail the written exam!
  - If written exam score is close to 40%, the weight of the home exam is reduced, i.e. only the written exam counts.

Digital written exam

- Digital exam, with a variety of question types, e.g.
  - Write text as answer
  - Fill in word / short text as answer
  - Fill in numerical value as answer
  - Select correct statement / multiple choice answers
- Related to lecture presentations and workshop questions.
  - Many workshop questions are not suitable as exam questions
- The digital exam has 10 sections, each worth 10 points.
  - Each section contains a small set of specific questions of 1-4 points
- 4 hours working time
  - Approx. 20 minutes for each section
- Good Luck ☺